



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,815	03/26/2004	Yoshihiro Hori	65933-083	7932
20277	7590	01/28/2009	EXAMINER	
MCDERMOTT WILL & EMERY LLP			LAFORGIA, CHRISTIAN A	
600 13TH STREET, N.W.				
WASHINGTON, DC 20005-3096			ART UNIT	PAPER NUMBER
			2439	
MAIL DATE		DELIVERY MODE		
01/28/2009		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/809,815	HORI ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Christian LaForgia	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 20 October 2008.  
 2a) This action is **FINAL**.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1,3-16 and 18 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1,3-16 and 18 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 26 March 2004 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_.  
 4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date \_\_\_\_\_.  
 5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_\_.

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 18 November 2008 has been entered.
2. Claims 1, 3-16 and 18 have been presented for examination.
3. Claims 2 and 17 have been cancelled as per Applicant's amendment.

### ***Response to Arguments***

4. Applicant's arguments with respect to claims 1, 3-16, and 18 have been considered but are moot in view of the new grounds of rejection set forth below.

### ***Claim Rejections - 35 USC § 103***

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
6. Claims 1, 3-5, 7, 8, 10-16, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 7,158,637 to Ohta et al., hereinafter Ohta, in view of U.S. Patent No. 4,238,854 to Ehrsam et al., hereinafter Ehrsam.
7. Regarding Claims 1 and 7, Ohta discloses a storage devices comprising:
  - a storage medium for retaining data (column 7 lines 43-53); and
  - a cryptographic processing unit (figure 3 Encryption and Authentication Processing Control Unit) which receives, from a host device, and executes a command corresponding to

each of the plurality of sequenced subprocesses produced by dividing each of a series of cryptographic input/output processes for encrypting data to be secured and inputting/outputting the data between the storage medium and the host device, (column 6 lines 1-20, and description of figure 3 particularly in column 6 lines 39-58),

wherein the cryptographic processing unit simultaneously processes subprocesses respectively belonging to two or more different cryptographic input and output processes by referring to identifying information attached to the command identifying to which cryptographic input/output process the command belongs (column 2 lines 7-11).

8. Ohta does not teach wherein the cryptographic processing unit manages the sequence of commands executed in each cryptographic input/output processing and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command.

9. Ehrsam discloses wherein the cryptographic processing unit manages the sequence of commands executed in each cryptographic input/output processing (column 14, lines 6-58, column 53, lines 11-59, column 58, lines 31-67) and issuing a procedural error when an incorrect sequence of commands is received (column 36, line 61 to column 37, line 13, column 80, line 3-67).

10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to manage the sequence of commands executed in each cryptographic input/output processing and reject the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command, since Ehrsam states at column 80, lines 3-7 that out of sequence commands or commands executed at the wrong time

would cause the destruction or loss of good data in the cryptoprocessors or provide useless data from the cryptoprocessors. Therefore, rejecting incorrectly sequenced commands ensures data integrity.

11. Regarding Claims 3 and 18, Ehrsam teaches teach the storage device and method wherein when the cryptographic processing unit receives the incorrectly sequenced command, the cryptographic processing unit interrupts the cryptographic input/output processing to which the command belongs (column 36, line 61 to column 37, line 13, column 80, line 3-67).

12. Regarding Claim 4 and 13, Ohta discloses the storage device and method according to claims 1 and 12, wherein the number of the cryptographic input/output processing which can be performed simultaneously by the storage device is predetermined in accordance with a performance of the storage device (column 2 lines 24-61 wherein the processing is achieved by breaking the data into predetermined data blocks according to the data block size for authentication processing).

13. Regarding Claims 5, 8, and 14, Ohta discloses the storage devices and method according to claim 1, 7, and 12 wherein in response to a request from the host device, the storage device provides to the host device the maximum number of cryptographic input/output processing which can be performed simultaneously by the storage device (column 2 lines 2-61 wherein the blocks are accumulated until the appropriate maximum size for the accumulation buffer then outputted).

14. As per claims 10 and 12, Ohta discloses a host device and method which exchanges data with a storage device that is capable of simultaneously performing a plurality of series of cryptographic input/output processes for encrypting data to be secured and inputting/outputting the data, the host device comprising:

a controller which divides the cryptographic input/output processing into a plurality of sequenced subprocesses and issues commands sequentially to the storage device thereby allowing the storage device to execute a subprocess to be executed on the storage device side (column 6 lines 1-20, and description of figure 3 particularly in column 6 lines 39-58); and

a cryptographic processing unit which carries out encryption or decryption that is required of the cryptographic input/output process (column 2 lines 7-11), wherein when the controller issues a command, the controller attaches identifying information to the command to identify to which one of the plurality of cryptographic input/output processes the command belongs (column 6 lines 1-20 where processing information is the identifying information).

15. Ohta does not teach wherein the cryptographic processing unit manages the sequence of commands executed in each cryptographic input/output processing and rejects the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command.

16. Ehrsam discloses wherein the cryptographic processing unit manages the sequence of commands executed in each cryptographic input/output processing (column 14, lines 6-58, column 53, lines 11-59, column 58, lines 31-67) and issuing a procedural error when an incorrect

sequence of commands is received (column 36, line 61 to column 37, line 13, column 80, line 3-67).

17. It would have been obvious to one of ordinary skill in the art at the time the invention was made to manage the sequence of commands executed in each cryptographic input/output processing and reject the execution of an incorrectly sequenced command when the cryptographic processing unit receives the incorrectly sequenced command, since Ehrsam states at column 80, lines 3-7 that out of sequence commands or commands executed at the wrong time would cause the destruction or loss of good data in the cryptoprocessors or provide useless data from the cryptoprocessors. Therefore, rejecting incorrectly sequenced commands ensures data integrity.

18. Regarding Claim 11, Ohta discloses the host device according to claim 10, wherein the controller issues a command to allocate a process system for performing the cryptographic input/output processing prior to initiation of the cryptographic input/output processing (column 6 lines 1-20 where processing information is the identifying information and the determination of which kind of processing the data requires is interpreted to be allocating a process system).

19. Regarding Claim 15, Ohta discloses the data input/output method according to claim 13, further comprising, prior to performing the cryptographic input/output processing, selecting and allocating identifying information for identifying the cryptographic input/output processing to be performed from among the prepared number of pieces of identifying information determined in

the determining step (column 6 lines 1-20 where processing information is the identifying information and the determination of which kind of processing the data requires is interpreted to be allocating a process system).

20. Regarding Claim 16, Ohta discloses the data input/output method according to claim 14, further comprising, prior to performing the cryptographic input/output processing, selecting and allocating identifying information for identifying the cryptographic input/output processing to be performed from among the prepared number of pieces of identifying information determined in the determining step (column 6 lines 1-20 where processing information is the identifying information and the determination of which kind of processing the data requires is interpreted to be allocating a process system).

21. Claims 6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ohta in view of Ehrsam applied above, and further in view U.S. Patent Application Publication No. 2003/0226029 A1 to Porter et al., hereinafter Porter.

22. Regarding claims 6 and 9, Ohta and Ehrsam do not teach the storage devices, wherein the storage medium comprises a normal data storing unit and a confidential data storing unit, the normal data storing unit storing normal data to be exchanged bypassing the cryptographic processing unit, the confidential data storing unit storing the secret data to be exchanged via the cryptographic processing unit.

23. Porter teaches the storage devices, wherein the storage medium comprises a normal data storing unit and a confidential data storing unit, the normal data storing unit storing normal data

to be exchanged bypassing the cryptographic processing unit, the confidential data storing unit storing the secret data to be exchanged via the cryptographic processing unit (Porter paragraph 39 common memory and protected memory).

24. It would be obvious to one of ordinary skill in the art at the time the invention was made to incorporate both a protected and common memory in the cryptographic system of Ohta, since Porter states in paragraph [0039] that a region of memory can be designated as protected from the unauthorized use by using encryption.

### ***Conclusion***

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

26. The following patents are cited to further show the state of the art with respect to cryptographic microprocessors, such as:

United States Patent No. 4,278,837 to Best, which is cited to show preventing hackers from executing instructions in the wrong sequence in cryptographic microprocessor.

United States Patent No. 4,465,901 to Best, which is cited to show preventing hackers from executing instructions in the wrong sequence in cryptographic microprocessor.

United States Patent No. 4,238,853 to Ehram et al., which is cited to show a patent related to one of the patents used to reject the claims of the instant application.

United States Patent No. 4,386,234 to Ehram et al., which is cited to show a patent related to one of the patents used to reject the claims of the instant application.

United States Patent No. 4,227,253 to Ehram et al., which is cited to show a patent related to one of the patents used to reject the claims of the instant application.

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

28. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

29. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/  
Primary Examiner, Art Unit 2439

clf